Lecture 1

Group theory is a fundamental part of mathematics. Groups crop up all over mathematics, physics, chemistry and so on. The reason they are so important is that they provide an abstract toolbox for understanding something absolutely fundamental: symmetry.

Just as Number Theory is the modern subject that grows from counting, Group Theory is the modern subject that grows from symmetry.

We will quickly revise the material from the first year, sometimes postponing proofs.

Definition 1. A *group* is a set G together with a binary operation

$$\circ : G \times G \to G$$

such that

Notice that the 'closure' axiom is contained in the statement that $\circ$ maps into G.

(A) $(x \circ y) \circ z = x \circ (y \circ z)$ for all $x, y, z \in G$;
(N) there is an element $e \in G$ with $e \circ g = g \circ e = g$ for all $g \in G$;
(I) for any $g \in G$ there is an element $h \in G$ with $h \circ g = g \circ h = e$.

Notice that (A) (the *associative property*) means that we can write 'products' of elements

$$g_1 \circ g_2 \circ \cdots \circ g_n$$

unambiguously (that is, the product is well-defined without the need to put in brackets to specify the order in which the binary operation is applied). The element h in G is usually called the *inverse* of g, and is written g^{-1} or $-g$ depending on whether we are writing the group operation multiplicatively or additively.

We will soon drop the $\circ$ and write xy for $x \circ y$.

There are some easy consequences of the definition.

Lemma 2. *The identity element e is unique: if e and e' both satisfy the property (N) then $e = e'$.*

Proof. Apply (N) with e' as g to see that

$$e \circ e' = e' \circ e = e'.$$

Now apply (N) with e as g and e' as the thing that satisfies (N) to see that

$$e' \circ e = e \circ e' = e.$$

It follows that $e = e'$. □

There are many similar things which we will use without comment.

Exercise 3. (1) Show that the inverse of an element is unique. That is, given $g \in G$ assume that h and h' satisfy (I) and prove that $h = h'$.
(2) [Cancellation Law] Prove that any equation $ax = b$ in a group (a and b are given and you must solve for x) always has exactly one solution.
(3) [Multiplication=Permutation] Prove that the map $\mathcal{L}_h : G \to G$ defined by $\mathcal{L}_h(g) = h \circ g$ is a *bijection*. This means that if I list the elements

of a group G in some order, then multiply by h on the left I get the *same list* of elements, possibly in a different order. That is, the map $\mathcal{L}_h$ is a *permutation* of the set G.
(4) Formulate and prove a similar statement for the map $\mathcal{R}_h : G \to G$ defined by $\mathcal{R}_h(g) = g \circ h$.

Examples are important in Group Theory and you should aim to become familiar with many different examples.

Example 4. The integers $\mathbb{Z}$ form a group under addition; this will be written $(\mathbb{Z}, +)$. This group is *abelian* and *cyclic*.

Niels Henrik Abel (1802–1829) was a Norwegian mathematician who proved that a fifth degree polynomial equation cannot be solved using radicals; he also contributed much to analysis and other parts of mathematics.

We will usually write abelian groups additively.

TABLE 1. Additive and Multiplicative notation.

additive	multiplicative
$x + y$	$x \circ y$ or xy
$-x$	x^{-1}
kx	x^k $(k \in \mathbb{Z})$

Definition 5. Let G be a group and $g \in G$ an element. The subgroup generated by g, denote $\langle g \rangle$, is the smallest subset of G that is a group and contains g. If we write g^n for $g \circ g \circ \cdots \circ g$ ($n \geqslant 1$ times), $g^0 = e$ and $g^{-n} = g^{-1} \circ g^{-1} \circ \cdots \circ g^{-1}$ ($n \geqslant 1$ times) then this may also be written

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}.$$

A group is called *cyclic* if there is an element g with $G = \langle g \rangle$. Any such element (there may be several) is called a *generator*.

Thus $(\mathbb{Z}, +)$ is cyclic because $\mathbb{Z} = \langle 1 \rangle$. The element -1 is also a generator.

Exercise 6. (1) Show that if g generates G then g^{-1} also generates G.
(2) Can you find a group with exactly one generator?
(3) Show that a cyclic group is abelian.

Example 7. [MODULAR ADDITION] Fix $n \geqslant 1$ and consider the numbers $\{0, 1, \ldots, n-1\}$ under addition modulo n. This is easily seen to be a group: the identity element is 0, the inverse of k is $n - k$, and addition is associative. Moreover, this group is generated by 1, so is cyclic and abelian. This group will be written $\mathbb{Z}/n\mathbb{Z}$ or C_n.

Taking $n = 6$ gives the group table shown in Table 2.

What about multiplication of integers? The integers under multiplication cannot be a group: multiplication by 0 violates the Cancellation Property. What about the non-zero integers? Multiplication by 1 acts like the identity so must be the identity. It follows that 2^{-1} would have to be $\frac{1}{2}$ which is not an integer. However, all is not lost...

TABLE 2. The group table of $\mathbb{Z}/6\mathbb{Z}$.

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Example 8. The set of non-zero integers under multiplication lives inside the group $(\mathbb{Q} \setminus \{0\}, \times)$.

A more subtle construction is to let R be a ring with a multiplicative identity 1 and write R^* for the set of elements of R with a multiplicative inverse. This always turns out to be a group, giving the following examples.

Example 9. The integers under multiplication (which of course does not form a group) contains a group, namely

$$(\mathbb{Z}, \times)^* = \{\pm 1\}.$$

Notice that this group is isomorphic to C_2.

We will have a precise definition of isomorphism later, but you should have already seen it.

Example 10. It makes sense to multiply integers modulo n, so what is

$$(\mathbb{Z}/n\mathbb{Z}, \times)^*?$$

This is not obvious, so take $n = 8$ and go through the elements $0, 1, \ldots, 7$ in turn and see if they have multiplicative inverses. We must exclude 0 because it violates the Cancellation Property. 1 looks fine, because $1 \times 1 = 1 \pmod 8$, so $1^{-1} = 1$. We must exclude 2, because $2 \times 2 \times 2 = 0 \pmod 8$, and we know 0 is not in the group. 3 looks fine, since $3 \times 3 = 1 \pmod 8$. Similarly 4 and 6 must be excluded, but 5 and 7 look fine.

Table 3 gives the group table for the group $(\mathbb{Z}/8\mathbb{Z}, \times)^*$. Notice that it is abelian but not cyclic. We will see this group again and it is sometimes called V_4.

TABLE 3. The group table of $(\mathbb{Z}/8\mathbb{Z}, \times)^*$.

$\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

The general picture is given by the following lemma, which you should have seen in Discrete Mathematics.

Lemma 11. *The elements of* $(\mathbb{Z}/n\mathbb{Z}, \times)^*$ *are those* m, $1 \leqslant m \leqslant n-1$ *with* $\gcd(m, n) = 1$.

Lecture 2

We continue with two more important examples. Each of these is an infinite family of groups.

Example 12. [Symmetric groups] The group S_n (also written Σ_n) is the group of all permutations of $\{1, 2, \ldots, n\}$. Notice that there are $n!$ elements in S_n. The first thing to do is to find a convenient notation for permutations, and one way to do this is using *cycle notation*.

Consider the permutation that sends 12345 to 42135. One way to write this is

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}.$$

Then, for example

$$p^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \text{ and } p^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix},$$

so p has *order* 3. The cycle notation for p just describes each *cycle*, in this case the cycles are shown in Figure 1.

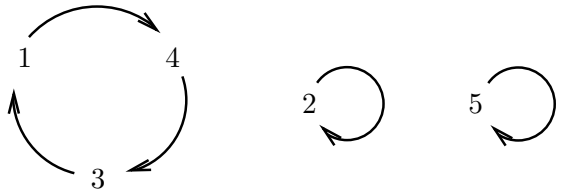

Figure 1. The cycles in p.

The cycle notation is then $p = (143)(2)(5)$. By convention, things that are fixed do not need to be mentioned, so we write $p = (143)$.

This makes it easy to multiply elements in symmetric groups, but the order matters. By pq we mean 'apply q then apply p' (that is, we think of permutations as acting like functions). You can think of feeding the numbers 1, 2, and so on in *from the right* to compute products. Thus

$$(123)(12) = (13)(2) = (13) \text{ and } (12)(123) = (1)(23) = (23).$$

In paticular, these groups are not abelian if $n \geqslant 3$.

Example 13. The elements of the group S_3 are $e, (12), (13), (23), (123), (132)$. For reasons that will become clear later, it makes sense to arrange these in the order shown in the group table shown in Table 4. Notice that the table falls naturally into four pieces as indicated.

Example 14. [Dihedral groups] The symmetries of any object – the rigid motions that move the object and return it to occupy the same space as before – automatically form a group. To see this, notice that the identity is always a symmetry, every symmetry has an inverse, the composition

TABLE 4. The group table of S_3.

	e	(123)	(132)	(12)	(13)	(23)
e	e	(123)	(132)	(12)	(13)	(23)
(123)	(123)	(132)	e	(13)	(23)	(12)
(132)	(132)	e	(123)	(23)	(12)	(13)
(12)	(12)	(23)	(13)	e	(132)	(123)
(13)	(13)	(12)	(23)	(123)	e	(132)
(23)	(23)	(13)	(12)	(132)	(123)	e

of two symmetries is a symmetry, and finally symmetries being maps are automatically associative.

A special class of groups are obtained from the symmetries of regular polygons. The dihedral group D_{2n} is the group of symmetries of a regular n-gon.

Example 15. Taking $n = 4$, the group D_8 may be found as follows. Let R denote rotation through $\pi/2$ anti-clockwise, and let T denote reflection in the vertical line. Notice (see Figure 2) that if we call the anti-clockwise order of the labels of the vertices, then R is orientation preserving and T is orientation reversing.

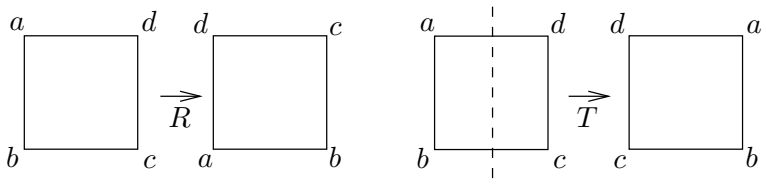

FIGURE 2. Rotation R and reflection T.

Any rigid motion must take the vertex a to one of 4 corners. The vertex b will then be sent to be one of its neighbours – its anti-clockwise neighbour if the motion is orientation preserving, its clockwise neighbour if not. Thus there are $4 \times 2 = 8$ elements in the group. We easily find that $e, R, R^2, R^3, RT, R^2T, R^3T$ are eight different motions, so they must be the elements of D_8. What about TR? A quick check reveals that $TR = R^3T$, and with this relation to hand anything can be written in the form R^iT^j with $i \in \{0, 1, 2, 3\}$ and $j \in \{0, 1\}$.

The group table for D_8 is shown in Table 5.

Finally, recall the following definitions.

If G and H are groups, then a *homomorphism* from G to H is a map

$$\phi : G \to H$$

with the property that $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$. A bijective homomorphism is called an *isomorphism*.

TABLE 5. The group table of D_8.

	e	R	R^2	R^3	T	RT	R^2T	R^3T
e	e	R	R^2	R^3	T	RT	R^2T	R^3T
R	R	R^2	R^3	e	RT	R^2T	R^3T	T
R^2	R^2	R^3	e	R	R^2T	R^3T	T	RT
R^3	R^3	e	R	R^2	R^3T	T	RT	R^2T
T	T	R^3T	R^2T	RT	e	R^3	R^2	R
RT	RT	T	R^3T	R^2T	R	e	R^3	R^2
R^2T	R^2T	RT	T	R^3T	R^2	R	e	R^3
R^3T	R^3T	R^2T	RT	T	R^3	R^2	R	e

A *subgroup* H of a group G is a subset that is itself a group and we will write $H \leqslant G$ for this.

The *order* of a finite group G is the number of elements in G, written $|G|$.

The *order* of an element $g \in G$, written $|g|$, is the size of the group $\langle g \rangle$ generated by g if this is finite.

Exercise 16. Draw the group table for D_6, the dihedral group of the triangle. Find an isomorphism between D_6 and S_3.

Lecture 3

We write $H \leqslant G$ to mean that H is a subgroup of G.

Exercise 17. Let G be a group. Prove that if $\emptyset \neq H \subset G$ (a non-empty subset) then H is a subgroup of G if and only if

$$x, y \in H \implies xy^{-1} \in H.$$

We wish to study how a group may be broken up into pieces by a subgroup.

Definition 18. Let H be a subgroup of G and let x be an element of G. The *right coset* of H by x is the set

$$Hx = \{hx \mid h \in H\}.$$

The *left coset* of H by x is the set

$$xH = \{xh \mid h \in H\}.$$

Example 19. Let $G = C_4 = \{1, g, g^2, g^3\}$, a cyclic group of order 4, and let $H = \{1, g^2\}$. Then

$$\begin{aligned} H1 &= \{1, g^2\} = H, \\ Hg &= \{g, g^3\}, \\ Hg^2 &= \{g^2, 1\} = H, \text{ and} \\ Hg^3 &= \{g^3, g^5 = g\} = Hg. \end{aligned}$$

'Partitions' just means chop into disjoint pieces.

Thus there are two cosets, H and Hg, and they *partition* G as shown in Figure 3.

1	g^2
g	g^3

Figure 3. The cosets of $\{1, g^2\}$ partition G.

Notice that Example 19 was an abelian group, so left and right cosets are the same.

Example 20. Let $G = \Sigma_3 = S_3 = \{e, (12), (13), (23), (123), (132)\}$, the symmetric group on 3 elements, and let $H = \{e, (23)\}$ be the subgroup of order 2 generated by (23). Then the right cosets of H are

$$\begin{aligned} He &= H, \\ H(123) &= \{(123), (13)\}, \\ H(132) &= \{(132), (12)\}, \\ H(23) &= \{(23), e\}, \\ H(31) &= \{(31), (123)\}, \text{ and} \\ H(12) &= \{(12), (132)\}. \end{aligned}$$

Notice that there are just three cosets, which we may choose to represent as H, $H(123)$ and $H(12)$. Once again the cosets partition the group as shown in Figure 4.

e	(132)	(123)
(23)	(12)	(13)

FIGURE 4. The cosets of H partition S_3.

Notice that the left cosets are different: for example $(123)H = \{(123), (12)\}$ is not equal to any right of the right cosets.

In both examples the same picture emerges:

- The cosets partition the group;
- Every coset has the same number of elements as H;

hence

- $|G| = |H| \times$the number of cosets.

This is *Lagrange's Theorem* which we prove next. Before doing so, it will be useful to quickly review the language of *equivalence relations*.

Definition 21. Let S be a set. A *relation* on S is a subset $R \subset S \times S$. We write aRb to mean $(a, b) \in R$.

This is an extremely general notion, as the following examples show.

(1) Let $R = \{(a, a) \mid a \in S\}$, the *diagonal*. Then the relation R is equality: aRb means $a = b$.
(2) Let $S = \mathbb{R}$ and $R = \{(x, y) \mid x < y\}$. Then aRb means that $a < b$.

We are interested in a very special sort of relation:

Definition 22. A relation R on a set S is called an *equivalence relation* if it is:

- **reflexive**, which means that xRx for all $x \in S$,
- **transitive**, which means that xRy and yRz implies xRz, and
- **symmetric**, which means that xRy implies yRx.

Exercise 23. The definition of equivalence relation looks redundant for the following reason: if a relation is symmetric and transitive, then surely xRy implies yRx, so xRx? What is wrong with that argument? Specifically, can you write down a relation that is symmetric and transitive but not reflexive?

We will always write equivalence relations with a tilde $\sim$, so $x \sim y$ means xRy. The importance of equivalence relations is that they are a natural way in which partitions arise.

Lemma 24. *If $\sim$ is an equivalence relation on S, then the equivalence classes*

$$[x]_\sim = \{y \in S \mid y \sim x\}$$

form a partition of S.

Proof. Each equivalence class is a set, and the lemma means that those sets are either disjoint or identical, and everything in S lies in one of them.

To see that the equivalence classes cover all of S is easy: given $x \in S$, we have $x \in [x]_\sim$ since $\sim$ is reflexive.

We now want to prove that if two equivalence classes are not identical sets, then they are disjoint.

It is enough to prove the *contrapositive* statement: if two equivalence classes are not disjoint, then they are identical. So assume that

$$[x]_\sim \cap [y]_\sim \neq \emptyset.$$

This means there is some z in $[x]_\sim$ and in $[y]_\sim$. So by symmetry $x \sim z$ and $z \sim y$, so by transitivity, $x \sim y$.

Now consider any $a \in [x]_\sim$. Then $a \sim x$; we know that $x \sim y$, so $a \sim y$ and hence $a \in [y]_\sim$. Thus $[x]_\sim \subset [y]_\sim$.

Similarly, consider any $b \in [y]_\sim$. Then $b \sim y$; we know that $y \sim x$ so $b \sim x$ and hence $b \in [x]_\sim$. Thus $[x]_\sim \supset [y]_\sim$. We conclude that $[x]_\sim = [y]_\sim$. $\square$

So anytime we find an equivalence relation we have a partition into disjoint sets. One of the most important examples is modular arithmetic.

Example 25. Define a relation $\sim$ on $\mathbb{Z}$ by $x \sim y$ if and only if $x \equiv y \pmod 3$. Then $\sim$ is an equivalence relation (easy exercise). The equivalence classes are

$$\begin{aligned} [0]_\sim &= \{\dots, -3, 0, 3, \dots\} = 3\mathbb{Z}, \\ [1]_\sim &= \{\dots, -2, 1, 4, \dots\} = 3\mathbb{Z} + 1, \text{ and} \\ [2]_\sim &= \{\dots, -1, 2, 5, \dots\} = 3\mathbb{Z} + 2. \end{aligned}$$

Notice that the same picture emerges: $\mathbb{Z}$ is the disjoint union of those three classes.

Exercise 26. Show that Lemma 24 has a converse. If a set S is partitioned into the disjoint union of subsets $A_1, A_3, \dots$ and I define a relation $\sim$ on S by $x \sim y$ if and only if x and y are in the same subset A_i, then $\sim$ is an equivalence relation, and the equivalence classes are the subsets $A_1, A_2, \dots$.

Theorem 27. [Lagrange's Theorem] *Let G be a finite group and $H \leqslant G$ a subgroup. Then the cosets of H all have the same number of elements, and they partition G. Hence*

$$|G| = |H| \times \textit{the number of cosets.}$$

Lecture 4

We will prove Lagrange's Theorem using the idea of equivalence relations. Let H be a subgroup of the finite group G, and define a relation $\sim$ on G by

$$\begin{aligned} x \sim y &\iff y \in Hx \\ &\iff y = hx \text{ for some } h \in H \\ &\iff yx^{-1} \in H. \end{aligned}$$

Claim one: $\sim$ is an equivalence relation.

- $\sim$ is **reflexive**: $x \sim x$ for any $x \in G$ since $xx^{-1} = e \in H$.
- $\sim$ is **transitive**: If $x \sim y$ and $y \sim z$ then yx^{-1} lies in H and zy^{-1} lies in H. Since H is a subgroup, it is closed under the group operation, so $zy^{-1}yx^{-1} = zx^{-1} \in H$, hence $x \sim z$.
- $\sim$ is **symmetric**: if $x \sim y$ then $yx^{-1} \in H$, so (since H is a group) $(yx^{-1})^{-1} = xy^{-1} \in H$, so $y \sim x$.

Notice we have used the important identity:

$$(ab)^{-1} = b^{-1}a^{-1},$$

which is valid in any group. By Lemma 24, it follows that the cosets of H partition G.

Claim two: The cosets all have the same number of elements.

In order to show this, it is enough to show that they all have the same number of elements as the special coset H itself. Define a map $\theta : H \to Hx$ by $h \mapsto hx$. This is clearly surjective (the elements of Hx are by definition things in the image of θ). If $\theta(h_1) = \theta(h_2)$ then $h_1x = h_2x$ so $h_1 = h_2$, showing that θ is injective.

We deduce that G is a disjoint union of cosets, all of which have the same number of elements, hence

$$|G| = |H| \times \text{the number of cosets.}$$

Thus in particular the order of H (the number of elements in H) divides the order of G. The integer $|G|/|H|$ is called the *index* of H in G, and it is sometimes written $[G : H]$.

Corollary 28. *Let G be a finite group.*

- *If $H \leqslant G$ then $|H|$ divides $|G|$.*
- *The order of $g \in G$ divides $|G|$.*
- *If $|G|$ is a prime number, then G is cyclic.*

Proof. If g has order m, then $< g >$ is a subgroup of G with order m, so m must divide G.

If $|G|$ is a prime p, then the order of any element $g \neq e$ must be p (it cannot be 1 and must divide p). So g generates a cyclic subgroup of order p, which must be all of G. □

This is the beginning of an intricate relationship between the *arithmetic* of the number $|G|$ and the *structure* of G. It turns out that complicated

numbers (many prime factors, or prime factors appearing to high powers) allow for more complicated possibilities.

Example 29. To get some idea of how much the arithmetic (not the size) of n influences the number of different (non-isomorphic) groups of order n, notice the following. There is exactly one group of order 255, but there are 56092 different groups of order 256.

Example 30. On a more reasonable scale, there is one group of order 15, and one group of order 17 — but there are 14 different groups of order 16; 5 abelian ones and 9 non-abelian ones.

For groups with a very special structure we can describe everything.

Theorem 31. [Subgroups of Cyclic Groups] *Let*

$$G = \{1, x, x^2, \ldots, x^{n-1}\}$$

be a cyclic group of order n. Then every subgroup of G is cyclic. For each d dividing n there is exactly one subgroup of G with order d, and it is generated by $x^{n/d}$.

Proof. Let H be a subgroup of G. By Lagrange's Theorem, $|H| = d$ must divide n. Write

$$H = \{1, h_1, \ldots, h_{d-1}\}.$$

Since $H \leqslant G$, each $h_i = x^{\lambda_i}$ for some λ_i, $0 < \lambda_i < n$. By Lagrange, the order of h_i divides d, so $h_i^d = 1$, and therefore $x^{d\lambda_i} = 1$ for all i. So $n | d\lambda_i$, and we may write

$$d\lambda_i = k_i n = k_i m d$$

for some integers m, k_i. Therefore $\lambda_i = k_i m$ where $m = n/d$, and

$$h_i = (x^m)^{k_i} \text{ for } i = 1, \ldots, d-1.$$

Thus every element of H is a power of x^m, so H is cyclic.

Now let d be any divisor of n. We claim that $x^{n/d}$ has order d. To see this, notice that

$$(x^{n/d})^k = 1 \implies \frac{nk}{d} | n \implies d | k,$$

so the least $k > 1$ with this property is d. It follows that $x^{n/d}$ generates a subgroup of order d. Uniqueness follows from the first argument: if H is any subgroup of order d then it is generated by $x^{n/d}$. □

We have seen several infinite families of finite groups:

- the **cyclic groups** $\{C_n \mid n \geqslant 1\}$,
- the **dihedral groups** $\{D_{2n} \mid n \geqslant 1\}$,
- the **symmetric groups** $\{S_n \mid n \geqslant 2\}$.

The next construction gives a new series,

- the **alternating groups** $\{A_n \mid n \geqslant 2\}$.

Fix $n \geqslant 2$ and let $x_1, \ldots, x_n$ be commuting variables. Write

$$\begin{aligned}\Delta_n &= (x_1 - x_2)(x_1 - x_3) \quad \cdots\cdots\cdots \quad (x_1 - x_n) \\ &\qquad \times (x_2 - x_3)(x_2 - x_4) \cdots (x_2 - x_n) \\ &\qquad\qquad \cdots \\ &\qquad\qquad\qquad \times (x_{n-1} - x_n).\end{aligned}$$

This can also be written as $\Delta_n = \prod_{n \geqslant j > i \geqslant 1} (x_i - x_j)$.

Example 32. $\Delta_2 = (x_1 - x_2)$, $\Delta_3 = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$.

Now let $\alpha \in S_n$ be a permutation and consider one term $(x_i - x_j)$ in Δ_n. If $\alpha(i) = \ell$ and $\alpha(j) = m$ then α acts on the suffixes to send $(x_i - x_j)$ to $(x_\ell - x_m)$.

Now $(x_\ell - x_m)$ is plus or minus one of the terms in Δ_n. Notice that this action of α on Δ_n will never produce the same term twice, since the suffixes in each term are different. It follows that α acting on the suffixes sends Δ_n to $\pm\Delta_n$.

Example 33. Let $n = 3$ and let $\alpha = (23)$. Then

$$\alpha(\Delta_3) = (x_1 - x_3)(x_1 - x_2)(x_3 - x_2) = -\Delta_3.$$

If $\beta = (123)$ then

$$\beta(\Delta_3) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = \Delta_3.$$

Definition 34. A permutation $\alpha \in S_n$ with $\alpha(\Delta_n) = \Delta_n$ is called *even*; one with $\alpha(\Delta_n) = -\Delta_n$ is called *odd*. The *sign* of α is $+1$ if α is even, and -1 if α is odd.

Theorem 35. *The map* $\operatorname{sign} : S_n \to \{\pm 1\}$ *is a homomorphism.*

Lecture 5

Proof. (of Theorem 35 Notice that $\{\pm 1\}$ is a group under multiplication. What the theorem means is that if $\alpha, \beta \in S_n$, then

$$\operatorname{sign}(\alpha\beta) = \operatorname{sign}(\alpha)\operatorname{sign}(\beta)$$

where $\alpha\beta$ denotes the composition of two permutations, and the product on the right-hand side is just the product of two real numbers.

What we need to check is that the way in which S_n *acts* on the terms in Δ_n is really an action: is the effect of applying β, then α, the same as the effect of applying $\alpha\beta$?

Consider a fixed term $(x_i - x_j)$:

$$(x_i - x_j) \xrightarrow{\beta} (x_{\beta(i)} - x_{\beta(j)}) \xrightarrow{\alpha} (x_{\alpha(\beta(i))} - x_{\alpha(\beta(j))}),$$

on the other hand

$$(x_i - x_j) \xrightarrow{\alpha\beta} (x_{(\alpha\beta)(i)} - x_{(\alpha\beta)(j)}).$$

Thus it is enough to check that $(\alpha\beta)(i) = \alpha(\beta(i))$ for each $i \in \{1, 2, \ldots, n\}$, and this is how the composition of two permutations was defined. □

Corollary 36. *The even permutations form a subgroup A_n of S_n. It is called the* alternating group on n symbols.

We will soon have a better and more general way to understand how homomorphisms relate to subgroups, but for now let's count the number of elements in A_n.

Lemma 37. *The number of elements in A_n ($n \geqslant 2$) is $\frac{1}{2}n!$.*

Proof. First notice that the permutation (12) is odd. It follows that the cosets $A_n e = A_n$ and $A_n(12)$ are different: $(12) \notin A_n$ but $(12) \in A_n(12)$.

Now let α be any permutation. If it is even, then $\alpha \in A_n$. If it is odd, then $\alpha(12)$ is even, so $\alpha(12) \in A_n$ and therefore $\alpha \in A_n(12)$.

We deduce that there are only two cosets of A_n, so S_n is the disjoint union,

$$S_n = A_n \bigsqcup A_n(12).$$

In particular, A_n has exactly half the number of elements of S_n. □

Example 38. The elements of A_3 are $\{e, (123), (132)\}$. The elements of A_4 are $\{e$, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)$\}$.

The symmetry group S_n gives the symmetries of n vertices with no structure. Imposing a structure on n vertices (a geometrical relationship) reduces the size of the group of symmetries.

Exercise 39. Label the vertices of a regular tetrahedron with the numbers $1, 2, 3, 4$. Show that the group of rigid motions (symmetries) of the tetrahedron is isomorphic to A_4. The motions (123) and (12)(34) are shown in Figure 5 as rotations about dashed lines (the heavy dots mark where the lines meet the faces of the tetrahedron).

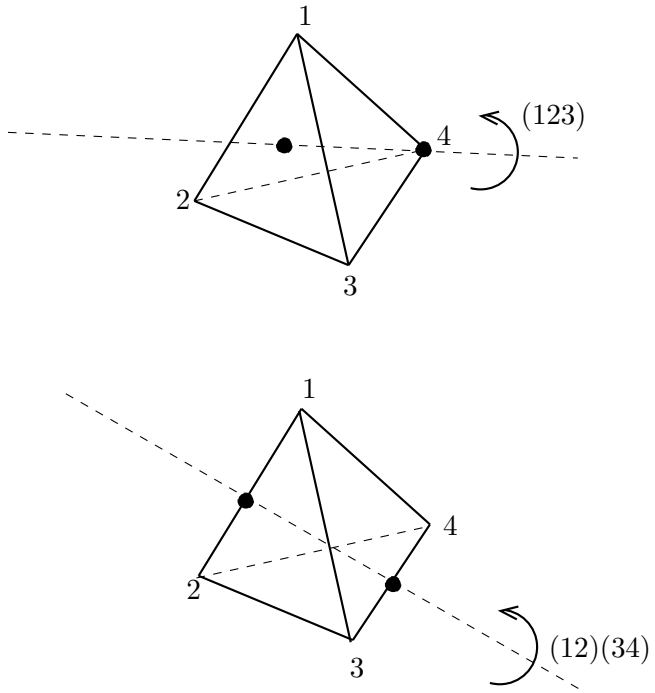

FIGURE 5. Two rigid motions of the tetrahedron.

Notice that (for example) the odd permutation (12) is not a motion of the tetrahedron. The last page of this lecture gives a graphic illustration of the three elements of order 2 and the eight elements of order 3 in A_4.

Normal subgroups and quotient groups

Recall Example 13, with the group table of S_3. The top left and bottom right quarters of the table only contain the elements $E = \{e, (123), (132)\}$ (which form a subgroup). The top right and bottom left corners only contain the elements $X = \{(12), (13), (23)\}$. The product of any element of E and any element of X is an element of X (and so on) so these two sets behave as show in Table 6.

So S_3 seems to give rise to two different groups: the subgroup E is easy to understand, but what about the group shown in Table 6? This looks like certain cosets of E forming a group isomorphic to C_2. There are two things to say about Table 6:

- It is expressing what happens when two cosets are multiplied together.

TABLE 6. The sets E and X in S_3.

	E	X
E	E	X
X	X	E

- It came about because we knew that sign is a homorphism.

The next step is to build on those two comments.

Definition 40. If A and B are subsets of a group G, then the product of A and B is defined to be the set

$$AB = \{ab \mid a \in A, b \in B\}.$$

We have seen some special cases: if A is a subgroup of G and $B = \{b\}$ contains a single element b, then $AB = Ab$ is the right coset of A by b.

Does it make sense to multiply cosets? This definition allows us to multiply any subsets, so we can certainly multiply cosets – but will the answer be another coset?

Example 41. If G is abelian and $H \leqslant G$, then the product of two cosets of H is always a coset of H:

$$\begin{aligned} (Ha)(Hb) &= (Ha)(bH) \text{ since } G \text{ is abelian} \\ &= H(ab)H \\ &= HH(ab) \text{ since } G \text{ is abelian} \\ &= H(ab) \text{ since } H \text{ is a subgroup.} \end{aligned}$$

In general, all I can say about $(Ha)(Hb)$ is that it is some subset of G – I need to be able to change Hb to bH in order to make sense of the product as a coset.

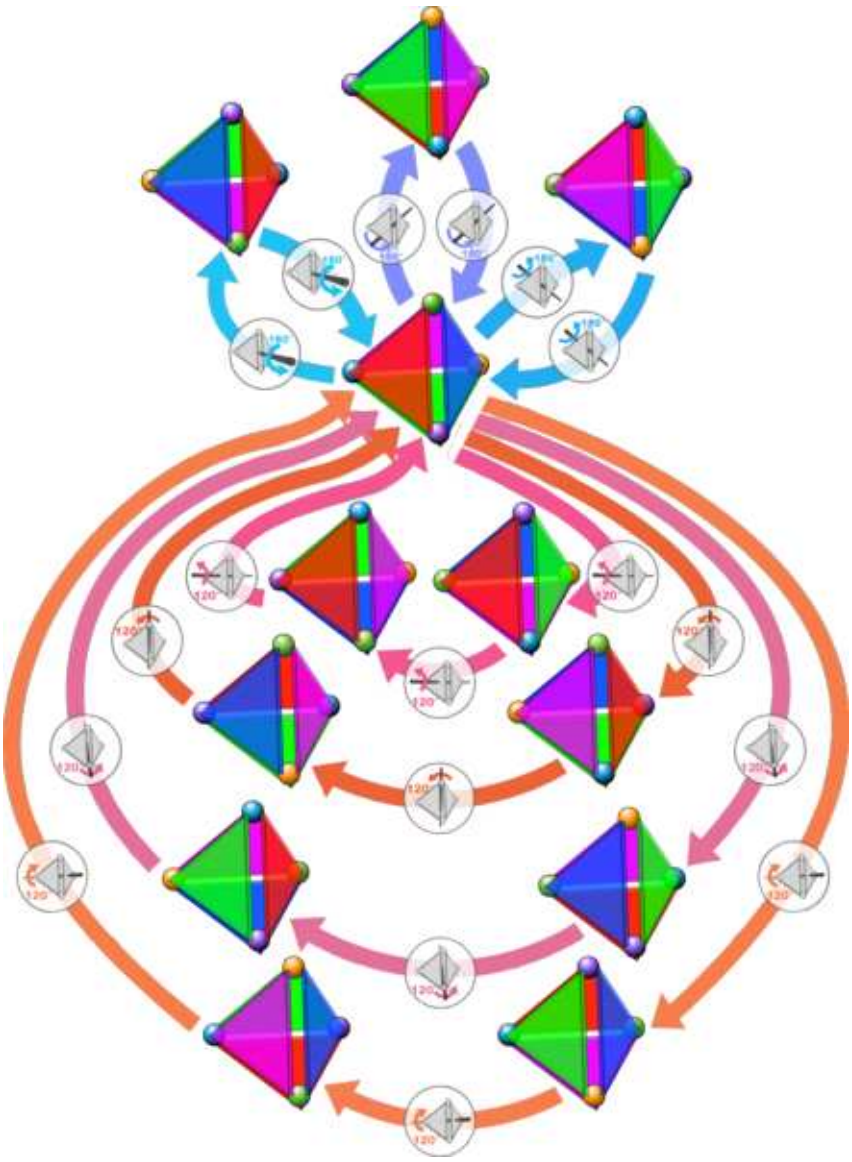

FIGURE 6. The symmetries of the tetrahedron.

LECTURE 6

We have seen that in an abelian group the product of two cosets is a coset. The next example shows this is not so in general.

Example 42. Consider the subgroup $H = \{e, (12)\}$ of the non-abelian group S_3. Then

$$H(123) = \{(123), (23)\}$$

and

$$H(132) = \{(132), (13)\}.$$

It follows that

$$H(123)H(132) = \{e, (12), (32), (123)\}$$

which is certainly not a coset of H (it has too many elements, for example).

Recall that what made cosets in an abelian group behave better than this was that Ha and aH were the same set.

Definition 43. A subgroup N of a group G is called *normal* if $Ng = gN$ for all $g \in G$. We denote normal subgroups by $N \lhd G$.

Notice that all subgroups of an abelian group are normal. The trivial subgroups $\{e\}$ and G are always normal.

Example 44. A_n is a normal subgroup of S_n for any $n \geqslant 2$. The clever way to prove this is to argue using the sign homomorphism. We know that there are only two cosets of A_n, namely A_n itself and $A_n(12)$. Now consider the coset $A_n g$. If g is odd, then $A_n g$ contains an odd element, so has an element in common with $A_n(12)$, so it must be $A_n(12)$. If g is even, then $A_n g = A_n$. Now consider gA_n: exactly the same argument shows that gA_n is $A_n(12)$ if g is odd, and is A_n if g is even. So $gA_n = A_n g$ for any g.

If $N \lhd G$ then write G/N for the *set of cosets* of N in G. Notice that Lagrange's Theorem shows that

$$\text{number of cosets } = |G/N| = |G|/|N|,$$

which makes the notation natural.

We are ready for the first big result of the course.

Theorem 45. *If $N \lhd G$ is a normal subgroup of G, then the set of cosets G/N is a group under the binary operation of multiplying cosets. This group is called a* quotient *or* factor *group and will sometimes be called G* modulo *N.*

Proof. First we should check that the statement makes sense: if I multiply two elements of G/N (two cosets of N) do I get another element of G/N?

Well,

$$\begin{aligned}(Na)(Nb) &= (Na)(bN) \text{ since } N \lhd G \\ &= N(ab)N \\ &= NN(ab) \text{ since } N \lhd G \\ &= Nab \text{ since } NN = N,\end{aligned}$$

so the binary operation is well-defined.

Now we need to check the group axioms.

Associativity:

$$[(Na)(Nb)]\,(Nc) = N(ab)c = Nabc \text{ since } G \text{ is a group;}$$

and

$$(Na)\,[(Nb)(Nc)] = Na(bc) = Nabc.$$

Neutral: $(Ne)(Na) = (Na)(Ne) = Na$, so the neutral is the subgroup N itself.
Inverses: $(Na)(Na^{-1}) = (Na^{-1})(Na) = Ne = N$.
Thus G/N is a group. □

We have already seen an example of this: S_3/E is the group C_2.

Example 46. We know that $A_n \lhd S_n$, and $|S_n/A_n| = 2$, so the quotient group must be isomorphic to C_2.

Example 47. Consider D_8 from Example 15, and let N denote the subgroup $\{e, R^2\}$. This is a subgroup since R has order 4. A calculation shows that $N \lhd D_8$ and $D_8/N \cong V_4$ as follows.

Recall that $D_8 = \{e, R, R^2, R^3, T, RT, R^2T, R^3T\}$. Clearly $gN = Ng$ if $g = R^j$ for some $j = 0, 1, 2, 3$. Now $TR = R^3T$, so $R^jTR^2 = TR^{f-j}R^2 = TR^{2-j} = R^{2+j}T$, so $gN = Ng$ for any $g \in D_8$. Thus $N \lhd D_8$.

To compute the quotient group, first identify the cosets:

$$D_8/N = \{N, NR, NT, NRT\}.$$

Now we find the relations:

$$\begin{aligned} (NR)^2 &= NR^2 = N; \\ (NT)^2 &= NT^2 = N; \\ (NRT)^2 &= N(RT)(RT) = N(RT)(TR^3) = N. \end{aligned}$$

So the quotient group has four elements, and every non-trivial element has order two – so it must be V_4.

Lecture 7

The easiest place to find normal subgroups is in an abelian group.

Exercise 48. Let $G = \mathbb{Z}$, the integers under addition. For each n the integers $n\mathbb{Z}$ divisible by n form a normal subgroup, and the quotient group $\mathbb{Z}/n\mathbb{Z}$ has n elements, given by the cosets

$$n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}.$$

The quotient group is a cyclic group, generated by the coset $1 + n\mathbb{Z}$.

If we write $0, 1, \ldots, (n-1)$ to denote the cosets we see that the quotient group is the integers modulo n under addition.

Where do normal subgroups come from?

Recall that we can think of the cosets of any subgroup as being like slices of a sliced loaf. If the subgroup happens to be a normal subgroup, then we know that the set of cosets is itself a group. There is a natural map that sends each element (crumb) to the coset (slice) it lives in. What kind of map is that?

Lemma 49. *If $N \lhd G$ is a normal subgroup, then the map*

$$\begin{aligned} \theta : G &\to G/N \\ g &\mapsto Ng \end{aligned}$$

is a surjective homomorphism of groups.

Surjective homomorphisms are also called *epimorphisms.*

Proof. Notice that θ sends the whole set N in G to the single element N in G/N. It is clearly surjective because the coset Ng is the image of $g \in G$.

To see it is a homomorphism, notice that

$$\theta(g_1 g_2) = N(g_1 g_2)$$

while

$$\begin{aligned} \theta(g_1)\theta(g_2) &= (Ng_1)(Ng_2) \\ &= N(g_1 g_2)N \text{ since } N \text{ is normal in } G \\ &= NN(g_1 g_2) \text{ since } N \text{ is normal in } G \\ &= N(g_1 g_2) \text{ since } N \text{ is a group,} \end{aligned}$$

so $\theta(g_1 g_2) = \theta(g_1)\theta(g_2)$. □

The next set of results show (among other things) that *all normal subgroups arise this way.* Any time you have a normal subgroup, it defines a homomorphism — and any time you have a homomorphism, it defines a normal subgroup.

Lemma 50. *Let $\theta : G \to H$ be a homomorphism between two groups. Then*

- *the* image *of θ,* $\mathrm{Im}(\theta) = \theta(G) = \{\theta(g) \mid g \in G\}$ *is a* subgroup *of H;*
- *the* kernel *of θ,* $\ker(\theta) = \{g \in G \mid \theta(g) = 1_H\}$ *is a* normal subgroup *of G.*

Proof. The image $\mathrm{Im}(\theta)$ is non-empty because $1_G \in G$ gets sent to

$$\theta(1_G) = 1_H \in \mathrm{Im}(\theta).$$

So it is enough to show that if h_1 and h_2 are in $\mathrm{Im}(\theta)$ then $h_1 h_2^{-1} \in \mathrm{Im}(\theta)$.

Well, if $h_1, h_2 \in \mathrm{Im}(\theta)$ then by definition there are elements $g_1, g_2 \in G$ with $\theta(g_1) = h_1$ and $\theta(g_2) = h_2$. Now $g_1 g_2^{-1} \in G$ (since G is a group) and

$$h_1 h_2^{-1} = \theta(g_1)\left(\theta(g_2)\right)^{-1} = \theta(g_1 g_2^{-1}) \in \mathrm{Im}(G)$$

since θ is a homomorphism. It follows that $\mathrm{Im}(\theta)$ is a subgroup of H.

Now consider the kernel. Again, this is non-empty since $1_G \in \ker(\theta)$. We use the same criteria to check that $\ker(\theta)$ is a subgroup: if $g_1, g_2 \in \ker(\theta)$ then

$$\begin{aligned} \theta(g_1 g_2^{-1}) &= \theta(g_1)\theta(g_2^{-1}) \\ &= \theta(g_1)\left(\theta(g_2)\right)^{-1} \\ &= 1_H 1_H^{-1} = 1_H, \end{aligned}$$

so $g_1 g_2^{-1} \in \ker(\theta)$, showing that $\ker(\theta)$ is a subgroup. Finally we want to show that $\ker(\theta)$ is a normal subgroup. Let $g \in G$ be any element and let $k \in \ker(\theta)$. Then

$$\begin{aligned} \theta(g^{-1}kg) &= \theta(g^{-1})\theta(k)\theta(g) \\ &= \left(\theta(g)\right)^{-1} 1_H \theta(g) \\ &= \left(\theta(g)\right)^{-1} \theta(g) = 1_H, \end{aligned}$$

so $g^{-1}kg \in \ker(\theta)$. It follows that $g^{-1}\ker(\theta)g \subset \ker(\theta)$, so

$$g^{-1}\ker(\theta)g = \ker(\theta),$$

showing that $\ker(\theta)$ is normal. □

Exercise: explain why $g^{-1}\ker(\theta)g \subset \ker(\theta)$ implies $g^{-1}\ker(\theta)g = \ker(\theta)$.

Lecture 8

The converse of Lemma 50 is also true.

Lemma 51. *If $N \lhd G$ is a normal subgroup, then the natural map*

$$\begin{aligned} \theta : G &\to G/N \\ g &\mapsto Ng \end{aligned}$$

has $\ker(\theta) = N$ *and* $\mathrm{Im}(\theta) = G/N$.

Proof. All that needs to be checked is that $Ng = N$ if and only if $g \in N$, and this is clear since $1_G \in N$. □

So the normal subgroups of a group G are exactly the kernels of homomorphisms from G.

Theorem 52. [First Isomorphism Theorem] *If $\theta : G \to H$ is any homomorphism of groups, then*

$$G/\ker(\theta) \cong \mathrm{Im}(\theta).$$

The symbol $\cong$ denotes an *isomorphism*, that is a bijective homomorphism.

Proof. This is easier to prove than it is to understand. The statement of the theorem goes as follows. As we know, $\ker(\theta)$ is a normal subgroup of G, so the coset space $G/\ker(\theta)$ is a group. The image $\mathrm{Im}(\theta)$ is a subgroup of H. Finally, there is an isomorphism between the group $G/\ker(\theta)$ and $\mathrm{Im}(\theta)$.

Write $K = \ker(\theta)$. Define a map ϕ from G/K to $\mathrm{Im}(\theta)$ as follows. An element of G/K is a coset Kg. Let's try to define

$$\phi(Kg) = \theta(g).$$

It is important to understand that this definition has a problem. Many different elements g could define the same coset – so does this definition really define anything?

I claim that the map ϕ is indeed *well defined*. If $Kg_1 = Kg_2$, then for some $k \in K$ we must have $g_1 = kg_2$. Hence

$$\theta(g_1) = \theta(kg_2) = \theta(k)\theta(g_2) = 1_H\theta(g_2) = \theta(g_2),$$

so that ϕ is function defined on the *cosets* not the individual choice of g.

Now check that ϕ is a homomorphism:

$$\begin{aligned} \phi(Kg_1Kg_2) &= \phi(Kg_1g_2) \text{ since } K \text{ is normal} \\ &= \theta(g_1g_2) \text{ by definition of } \phi \\ &= \theta(g_1)\theta(g_2) \text{ since } \theta \text{ is a homomorphism} \\ &= \phi(Kg_1)\phi(Kg_2) \text{ by definition of } \phi. \end{aligned}$$

Finally, we check that ϕ is a bijection.

It is clear that ϕ is surjective: an element of $\mathrm{Im}(\theta)$ is *by definition* something of the form $\theta(g)$ for some $g \in G$. Then $\phi(Kg) = \theta(g)$, showing that ϕ is surjective.

If $\phi(Kg_1) = \phi(Kg_2)$ then $\theta(g_1) = \theta(g_2)$, so

$$1_H = \theta(g_1)\left(\theta(g_2)\right)^{-1} = \theta(g_1g_2^{-1}),$$

showing that $g_1 g_2^{-1} \in K$, which in turn implies that $Kg_1 = Kg_2$. That is, $\phi(Kg_1) = \phi(Kg_2)$ implies that $Kg_1 = Kg_2$, showing that ϕ is injective. □

Exercise 53. Let $N \lhd G$ be a normal subgroup, and let $H \leqslant G$ be any subgroup with $N \leqslant H \leqslant G$. Show that $N \lhd H$ and show that H/N is a subgroup of G/N. Finally, show that every subgroup of G/N has the form H/N for some subgroup H with $N \leqslant H \leqslant G$.

Example 54. It may be helpful to see what the First Isomorphism Theorem looks like in a vague example, where we just show the number of elements as in Figure 7.

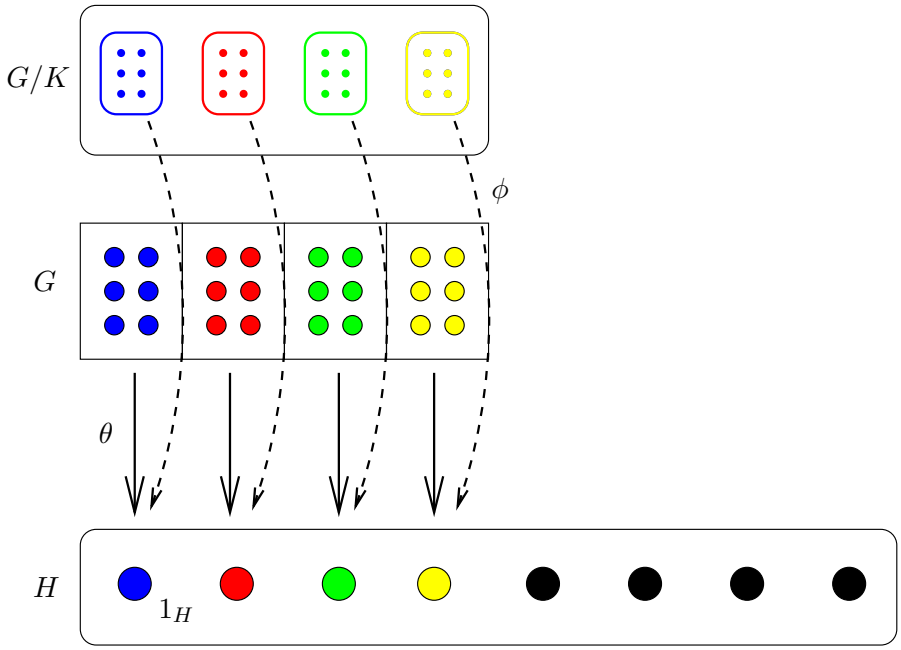

FIGURE 7. An illustration of the First Isomorphism Theorem.

Imagine a group G with 24 elements and a homomorphism

$$\theta : G \to H$$

into a group H with eight elements. The homomorphism is not surjective: the image of θ consists of the blue, red, yellow and green elements in H, while the four black ones are not in the image. The homomorphism is not injective: all the elements of one colour get sent to the same element of H. Thus θ is a 6-to-1 map.

The kernel K of θ is the blue subgroup, and the cosets of the kernel are the four blocks of single colours in G.

We are given the map θ shown in bold. There are two difficult things to understand about the First Isomorphism Theorem. Firstly, what is G/K?

That is the group with four elements, each of which is a coset of K. Second, how is the map ϕ constructed? This is shown with a dotted arrow in Figure 7.

The confusing part of the proof is the beginning. In order to write down the map ϕ I seem to need to make a choice. In order to write down the image of the red element of G/K under ϕ, I need to choose one of 6 elements of G, so it looks like there could be several possible images. However, because the elements of G/K are cosets of the kernel of θ, all those six elements get sent to the same place. This makes ϕ well-defined and the rest follows.

Lecture 9

Groups acting on sets

So far we have studied groups in an abstract way (though many of the groups were constructed as sets of symmetries or sets of permutations). One of the most important ideas in group theory is to extend the process and study how groups act on things. It will turn out that we have already seen many examples of this.

Definition 55. Let G be a group and let X be a non-empty set. We say that G *acts on* X if for each $x \in X$ and $g \in G$ there corresponds an element written $gx \in X$ in such a way that

- $g_2(g_1x) = (g_2g_1)x$ for all $x \in X$, $g_1, g_2 \in G$;
- $ex = x$ for all $x \in X$ where e is the identity in G.

Thus a group action is a map

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto gx \end{aligned}$$

with certain properties.

Notice that the property defining a group action is quite subtle: what it means is

$$\underbrace{g_2(\overbrace{g_1x}^{g_1 \text{ acts on } x})}_{g_2 \text{ acts on } g_1x} = \underbrace{\overbrace{(g_2g_1)}^{\text{product in } G}x}_{g_1g_2 \text{ acts on } x}$$

for all $x \in X$ and $g_1, g_2 \in G$.

Example 56. The idea of a group action is quite general, as the following examples show.

(1) [Permutation groups] For any set X let S_X be the group of all permutations of X, and let G be any subgroup of S_X. Then G acts on X by defining

$$gx = \text{image of } x \text{ under the permutation } g \in G.$$

Notice that $g_2(g_1x) = (g_2g_1)x$ is the definition of composition of maps (a permutation of X is a bijection $X \to X$). Also $ex = x$ since the group identity e is the identity permutation.

(2) [Action on cosets] Let $H \leqslant G$ be any subgroup of a group G. Let $X = \{aH \mid a \in G\}$ be the space of left cosets of H. Then for any $g \in G$ and $aH \in X$, the set gaH is a left coset of H so $gaH \in X$. This defines an action of G on X:

$$\begin{aligned} g_2(g_1aH) &= g_2g_1aH \text{ by the associative law in } G \\ &= (g_2g_1)aH, \end{aligned}$$

and $e(aH) = (ea)H = aH$.

(3) [CONJUGATION] Let G be a group and let $X = G$ as a set. Then there is an action of G on X by *conjugation* defined as follows. Define the element given by the action of $g \in G$ on $x \in X$ to be $gxg^{-1} \in X$. It would be very confusing to denote this by gx, so we follow a convention that writes this as ${}^{g}x$. Thus we claim that

$$ {}^{g}x = gxg^{-1} $$

defines an action of G on X. We need to check the two axioms for an action:

$$\begin{aligned} {}^{g_2}({}^{g_1}x) &= {}^{g_2}\left(g_1 x g_1^{-1}\right) \\ &= g_2(g_1 x g_1^{-1})g_2^{-1} \\ &= g_2 g_1 x g_1^{-1} g_2^{-1} \text{ by the associative law in } G. \end{aligned}$$

On the other hand

$$\begin{aligned} {}^{(g_2 g_1)}x &= g_2 g_1 x (g_2 g_1)^{-1} \\ &= g_2 g_1 x g_1^{-1} g_2^{-1} = {}^{g_2}({}^{g_1}x) \end{aligned}$$

so

$$ {}^{g_2}\left({}^{g_1}x\right) = {}^{(g_2 g_1)}\, x. $$

Clearly ${}^{e}x = exe^{-1} = x$, so this is an action.

Lecture 10

The next result is important and easy – but very confusing. Just as we saw that normal subgroups and kernels of homomorphisms are more or less the same things, it turns out that group actions and permutations are more or less the same things.

Theorem 57. *Let G act on a set X.*

- *For each $g \in G$ the map $\lambda_g : X \to X$ defined by $\lambda_g(x) = gx$ is a permutation of X (and so is a member of the symmetric group S_X).*
- *The map $\lambda : G \to S_X$ defined by $\lambda(g) = \lambda_g$ is a homomorphism.*

Proof. We need to show that λ_g is a bijection of X. Fix $g \in G$ and let $x, y \in X$. Then

$$\begin{aligned} \lambda_g(x) &= \lambda_g(y) \\ \implies gx &= gy \\ \implies g^{-1}(gx) &= g^{-1}(gy) \\ \implies (g^{-1}g)x &= (g^{-1}g)y \text{ by first axiom of 'action'} \\ \implies ex &= ey \\ \implies x &= y \text{ by second axiom of 'action'} \end{aligned}$$

so λ_g is injective. Also, for any $x \in X$,

$$\lambda_g(g^{-1}x) = g(g^{-1}x) = ex = x,$$

so λ_g is surjective. Hence λ_g is a permutation of X for each $g \in G$, which we write as $\lambda_g \in S_X$.

For the second part, we know that $g \mapsto \lambda_g$ is indeed a map from G to S_X. To see that it is a homomorphism,

$$\begin{aligned} \lambda_{\underbrace{g_1 g_2}_{\text{in } G}}(x) &= (g_1 g_2)x \text{ by definition of } \lambda \\ &= g_1(g_2 x) \text{ by first axiom of 'action'} \\ &= \lambda_{g_1}\left(\lambda_{g_2}(x)\right) \text{ by definition of } \lambda \\ &= \underbrace{(\lambda_{g_1}\lambda_{g_2})}_{\text{in } S_X}(x), \end{aligned}$$

and elements of S_X are equal if they do the same thing to each $x \in X$, so

$$\lambda(g_1 g_2) = \lambda_{g_1 g_2} = \lambda_{g_1}\lambda_{g_2} = \lambda(g_1)\lambda(g_2)$$

and λ is a homomorphism. □

Thus *an action defines a homomorphism to the group of permutations of the set acted on.* The converse is also true.

Theorem 58. *Let X be a non-empty set and G a group. Assume that we have a homomorphism $\lambda : G \to S_X$. Then the definition*

$$gx = \lambda(g)(x)$$

defines an action of G on X.

Proof. This is an easy exercise. □

Actions also define equivalence relations (and therefore partitions).

Lemma 59. *Let G act on a set X. Define a relation $\sim$ on X by saying that $x \sim y$ if and only if there is some $g \in G$ with $gx = y$. Then $\sim$ is an equivalence relation on X.*

Proof. One of the axioms of a group action says that $ex = x$ for all $x \in X$, so $x \sim x$ for all $x \in X$ and $\sim$ is reflexive.

If $x \sim y$ then there is some $g \in G$ with $gx = y$. Now

$$\begin{aligned} g^{-1}(gx) &= (g^{-1}g)x \text{ by the first part of Definition 55} \\ &= ex = x \text{ by the second part} \end{aligned}$$

so $x = g^{-1}y$ and therefore $y \sim x$, showing that $\sim$ is symmetric.

Finally, if $x \sim y$ and $y \sim z$ then there are elements $g_1, g_2 \in G$ with $x = g_1 y$ and $y = g_2 z$ so

$$x = g_1(g_2 z) = (g_1 g_2)z,$$

showing that $x \sim z$ so $\sim$ is transitive. □

Thus if G acts on a set X then X is partitioned into disjoint equivalence classes. These classes are called the *orbits* of the action, and for each $x \in X$ the equivalence class containing x is called the orbit of x.

Theorem 60. *Let G act on a set X and let $x \in X$. Write*

$$\mathrm{Stab}_G(x) = \{g \in G \mid gx = x\}$$

for the stabilizer *of x. Then $\mathrm{Stab}_G(x)$ is a subgroup of G.*

Proof. We know that $ex = x$ so $e \in \mathrm{Stab}_G(x)$ and thus $\mathrm{Stab}_G(x)$ is not empty.

If $g_1, g_2 \in \mathrm{Stab}_G(x)$ then $g_1 x = g_2 x = x$, so

$$\begin{aligned} g_2^{-1}(g_2 x) &= g_2^{-1}x \\ \therefore (g_2^{-1}g_2)x &= g_2^{-1}x \\ \therefore ex &= g_2^{-1}x \\ \therefore g_2^{-1}x &= x, \end{aligned}$$

so $g_2^{-1} \in \mathrm{Stab}_G(x)$. Thus

$$(g_1 g_2^{-1})x = g_1(g_2^{-1}x) = g_1 x = x$$

so $g_2 g_2^{-1} \in \mathrm{Stab}_G(x)$, showing it is a subgroup of G. □

Example 61. Let H be a subgroup of G. Then H acts on G (think of G as the set X) by left multiplication: the element $h \in H$ sends g to hg.

The orbit of g is the set Hg, a coset of H.

The stabiliser of g is $\{e\}$.

Now if the *stabiliser* of x is very big (all of G for example), then the *orbit* of x must be small. Similarly, if the stabiliser is small then most elements of G move x, so the orbit should be big. The next result makes this precise.

Theorem 62. *Let G act on a set X and fix $x \in X$. Then the number of elements in the orbit of x is the index of $\mathrm{Stab}_G(x)$ in G. In symbols,*

$$|\textit{orbit of } x| = |Gx| = |G|/|\mathrm{Stab}_G(x)|.$$

Proof. Let $X_1 = \{gx \mid g \in G\}$ be the orbit of x, $H = \mathrm{Stab}_G(x)$ and $Y = G/\mathrm{Stab}_G(x)$ (the set of cosets – this is not a group since we have no reason to expect the stabiliser to be a normal subgroup).

We wish to show that $|X_1| = |Y|$, and we do this by finding a bijection between them. Define a map $\mu : X_1 \to Y$ by $\mu(gx) = gH$. Notice we have a familiar problem: gx is a point on the orbit of x, but there could be many different gs that give the same point. For example, any $g \in \mathrm{Stab}_G(x)$ has $gx = x$. So the first thing is to check that the map is well-defined. Pick $g_1, g_2 \in G$ with $g_1x = g_2x$. Then

$$g_2^{-1}(g_1x) = x \implies g_2^{-1}g_1 \in H \implies g_2H = g_1H,$$

so the map μ is well-defined.

The map μ is surjective by definition: just start with the g you want.

We claim that μ is injective:

$$\begin{aligned} g_1H &= g_2H \\ \implies g_2^{-1}g_1H &= H \\ \implies g_2^{-1}g_1 &\in H \\ \implies (g_2^1g_1)x &= x \\ \implies g_1x &= g_2x, \end{aligned}$$

so μ is injective and surjective. □

This is the first of several important results that relate group actions to counting problems. We will give just one application.

Counting orbits under conjugation

Recall the conjugation action ${}^gx = gxg^{-1}$ of any group on itself. The element gxg^{-1} is called a *conjugate* of x, and the orbit

$$\{gxg^{-1} \mid g \in G\}$$

is called the *conjugacy class* of x. Thus G is partitioned into disjoint *conjugacy classes*.

If G is abelian, then each of these classes consists of a single element. The size of these clases tells you how far away from being abelian a group is.

The stabilizers under this action look like

$$\mathrm{Stab}_G(x) = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}.$$

This is usually called the *centralizer* of x, written $C_G(x)$.

Exercise 63. The centralizer $C_G(x) = \{g \in G \mid gx = xg\}$ is a subgroup of G.

We can now apply the general results about group actions.

Corollary 64. *For each $x \in G$, the number of conjugates of x is equal to $|G|/|C_G(x)|$.*

This is just Theorem 62 in disguise: the conjugates of x are the orbit of x, and the centralizer of x is the stabiliser of x.

This is a non-trivial fact about groups: the centralizers of conjugate elements have the same index.

Example 65. Let $G = S_3$, and consider the element $x = (123)$. Since conjugate elements always have the same order (easy exercise), the only possible conjugates of x are the elements of order three, (132) and (123). We check that

$$exe^{-1} = x, (12)x(12)^{-1} = (12)(123)(12) = (132),$$

so the conjugates of x are x itself and $x^{-1} = (132)$.

A calculation shows that

$$C_G(x) = \{e, x, x^{-1}\} = A_3,$$

so $|G|/|C_G(x)| = 2$ as expected.

Corollary 66. [The Class Equation] *If G is a finite group with k conjugacy classes, and if $x_1, \ldots, x_k$ are elements of G chosen one from each of the conjugacy classes, then*

$$|G| = |G|/|C_G(x_1)| + \cdots + |G|/|C_G(x_k)|.$$

This gives the second result relating the arithmetic of $|G|$ to the structure of G.

Theorem 67. *If p is a prime, then any group of order p^2 is abelian.*

Proof. In the notation of the Class Equation, we have

$$p^2 = m_1 + \cdots + m_k \tag{1}$$

where each $m_i = |G|/|C_G(x_i)|$. By Lagrange's Theorem, each m_i divides p^2 since p^2/m_i is the size of the subgroup $C_G(x_i)$.

On the other hand, the conjugacy class of e is automatically just $\{e\}$, so one of the m_i (let us say m_1) must be 1.

It follows that no m_i can be p^2, so they must all be 1 or p.

Reducing (1) modulo p shows that some other term m_j with $j \geqslant 2$ say must be 1. Thus

$$gx_jg^{-1} = x_j \text{ for all } g \in G. \tag{2}$$

Suppose that G is NOT abelian: there is some $a \in G$ with

$$gag^{-1} \neq a. \tag{3}$$

Then we must have $|G|/|C_G(a)| = p$ since it cannot be 1. Hence by Lagrange again, $|C_G(a)| = p$ so $C_G(a)$ is a *cyclic* group, and we may write

$$C_G(a) = \{e, a, a^2, a^3, \ldots, a^{p-1}\}.$$

By (2) we know $ax_ja^{-1} = x_j$, so $ax_j = x_ja$ and $x_j \in C_G(a)$. Hence (since p is a prime number) we must have

$$C_G(a) = \{e, x_j, x_j^2, dots, x_j^{p-1}\}$$

and in particular $a = x_j^\ell$ for some ℓ. It follows that

$$a = x_j^\ell = (gxg^{-1})^\ell = gx_j^\ell g^{-1} = gag^{-1}$$

which contradicts (3). So the group must be abelian. □

Exercise 68. Deduce from this that a group of order p^2 is either the cyclic group C_{p^2} or the product $C_p \times C_p$.